



HTTP Request Smuggling via Chunked Extension Quoted-String Parsing

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-2332
State	PUBLISHED
Assigner	eclipse
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 12:16:21 UTC
Updated	2026-04-14 12:16:21 UTC

Description In Eclipse Jetty, the HTTP/1.1 parser is vulnerable to request smuggling when chunk extensions are used, similar to the "fu

Risk And Classification

Primary CVSS: v3.1 7.4 HIGH from emo@eclipse.org

CVSS: 3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

EPSS: 0.000310000 probability, percentile 0.087050000 (date 2026-04-14)

Problem Types: CWE-444 | CWE-444 CWE-444 Inconsistent interpretation of HTTP requests ('HTTP Request/Response smuggling')

Version	Source	Type	Score	Severity	Vector
3.1	emo@eclipse.org	Secondary	7.4	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	7.4	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Eclipse Foundation	Eclipse Jetty	affected 12.1.0 12.1.6 semver	Not specified
CNA	Eclipse Foundation	Eclipse Jetty	affected 12.0.0 12.0.32 semver	Not specified
CNA	Eclipse Foundation	Eclipse Jetty	affected 11.0.0 11.0.27 semver	Not specified
CNA	Eclipse Foundation	Eclipse Jetty	affected 10.0.0 10.0.27 semver	Not specified
CNA	Eclipse Foundation	Eclipse Jetty	affected 9.4.0 9.4.59 semver	Not specified

References

Reference	Source	Link	Tags
github.com/jetty/jetty.project/security/advisories/GHSA-355h-qmc2-wpwf	emo@eclipse.org	github.com	
gitlab.eclipse.org/security/cve-assignment/-/issues/89	emo@eclipse.org	gitlab.eclipse.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: <https://github.com/xclow3n> (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report